Mathematik

Untersuchungen über ungerade vollkommene Zahlen

Inaugural-Dissertation

zur Erlangung des Doktorgrades
bei der Naturwissenschaftlichen Fakultät der
Schlesischen Friedrich-Wilhelms-Universität
zu Breslau

Vorgelegt von

Hans-Joachim Kanold

aus Breslau

Breslau 1941

Druck von Walter de Gruyter & Co. Berlin

Mathematik

Untersuchungen über ungerade vollkommene Zahlen

Inaugural-Dissertation

zur Erlangung des Doktorgrades
bei der Naturwissenschaftlichen Fakultät der
Schlesischen Friedrich-Wilhelms-Universität
zu Breslau

Vorgelegt von

Hans-Joachim Kanold

aus Breslau

Breslau 1941

Druck von Walter de Gruyter & Co. Berlin

D 2

Referent: Prof. Dr. Feigl

Korreferent: Prof. Dr. Radon

Examen rigorosum: 20. September 1939

Gedruckt mit Genehmigung der Naturwissenschaftlichen Fakultät der Schlesischen Friedrich-Wilhelms-Universität zu Breslau

Erscheint im Journal für die reine und angewandte Mathematik, Bd. 183, Heft 2, 1941.

Bezeichnet man die Summe der Teiler einer positiven ganzen Zahl n, einschließlich 1 und n, mit $\sigma(n)$, so heißt n vollkommen, wenn $\sigma(n) = 2n$ ist. Über die ungeraden vollkommenen Zahlen herrscht noch völlige Unklarheit: Weder ist ein Beispiel einer solchen Zahl, noch ein Satz über ihre Existenz oder Nichtexistenz bekannt. Bekannt sind lediglich notwendige Bedingungen für die Struktur der Primfaktorenzerlegung einer ungeraden vollkommenen Zahl.

Schon Euler [1]) hat bewiesen, daß die Zerlegung die Gestalt $n = p^{\alpha} q_1^{2\beta_1} \cdots q_r^{2\beta_r}$ mit $p \equiv \alpha \equiv 1 \pmod 4$ hat. In der vorliegenden Arbeit werden in I einige Aussagen über Kreisteilungspolynome bewiesen; insbesondere wird ein Satz von Kronecker [2]) verschärft und auf neue Art hergeleitet. In Anwendung dieses Satzes ergibt sich in II, daß der größte in einer ungeraden vollkommenen Zahl n aufgehende Primteiler mindestens doppelt so groß ist wie der größte der um 1 vermehrten Exponenten in der Primzahlzerlegung von n. Das Ergebnis von III besagt, daß n durch t^4 teilbar ist, wenn t den größten gemeinsamen Teiler der um 1 vermehrten geraden Exponenten in der Primfaktorenzerlegung von n bedeutet. Hieraus ergeben sich in IV weitere notwendige Bedingungen für die Existenz ungerader vollkommener Zahlen; z. B. ist n nicht vollkommen, wenn alle um 1 vermehrten geraden Exponenten durch 9 teilbar sind.

I. Sätze über Kreisteilungspolynome.

Wir wollen unter dem m-ten Kreisteilungspolynom $F_m(x)$ jenes ganzzahlige, normierte, in bezug auf den Körper P der rationalen Zahlen unzerlegbare Polynom verstehen, dessen Wurzeln genau die primitiven m-ten Einheitswurzeln $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\varphi(m)}$ sind. Es ist also

$$F_m(x) = (x - \varepsilon_1)(x - \varepsilon_2) \cdots (x - \varepsilon_{\varphi(m)}). \tag{1}$$

Betrachtet man $F_m(x)$ an allen ganzen rationalen Stellen x, so gilt nach Kronecker [3]): Ist r ein Primteiler vom $F_m(x)$, so ist entweder $r \mid m$ oder $r \equiv 1 \pmod m$. Es soll nun dieser Satz verschärft und auf andere Weise bewiesen werden.

(2) **Satz.** *Ist* $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \geqq 3$ *mit* $p_1 < p_2 < \cdots < p_k$ *und* x *eine ganze rationale Zahl, ist ferner* r *ein Primteiler von* $F_m(x)$, *so ist die Bedingung* $p_k \equiv 1 \pmod{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{k-1}^{\alpha_{k-1}}}$ *notwendig dafür, daß* $r = p_k$, *und die Bedingung*

[1]) L. Euler, Opera posthuma I, S. 14—15; vgl. auch L. E. Dickson, History of the theory of numbers **1**, S. 19.

[2]) L. Kronecker, Gesammelte Werke **3**, 1, S. 281—292. Vgl. auch Monatsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin 1888, S. 417—423.

[3]) Vgl. Fußnote [2]).

$p_k \not\equiv 1 \pmod{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{k-1}^{\alpha_{k-1}}}$ *hinreichend dafür, daß* $r \equiv 1 \pmod{m}$ *ist. Ferner gilt: Im Falle* $p_k \mid F_m(x)$ *ist* $p_k^2 \nmid F_m(x)$.

Beweis. Es ist

$$\frac{x^m - 1}{x - 1} = 1 + x + x^2 + \cdots + x^{m-1} = F_m(x) \cdot \prod_{d \mid m;\, d \neq 1,\, \neq m} F_d(x). \tag{3}$$

Setzt man $\frac{m}{p_\varkappa} = m_\varkappa$ $(\varkappa = 1, 2, \ldots, k)$, so ist

$$1 + x + \cdots + x^{m-1} = (1 + x + x^2 + \cdots + x^{m_\varkappa - 1})(1 + x^{m_\varkappa} + x^{2m_\varkappa} + \cdots + x^{(p_\varkappa - 1)m_\varkappa}). \tag{4}$$

Setzt man ferner zur Abkürzung

$$1 + x + x^2 + \cdots + x^{m_\varkappa - 1} = a_\varkappa, \tag{5}$$

$$1 + x^{m_\varkappa} + x^{2m_\varkappa} + \cdots + x^{(p_\varkappa - 1)m_\varkappa} = b_\varkappa,$$

so sieht man aus (3) und (4), daß

$$F_m(x) \mid b_\varkappa \qquad (\varkappa = 1, \ldots, k) \tag{6}$$

ist. Es sei nun

$$r_\varkappa \mid b_\varkappa \tag{7}$$

und $r_\varkappa$ eine Primzahl. Dann ist

$$x^m = x^{m_\varkappa p_\varkappa} \equiv 1 \pmod{r_\varkappa}. \tag{8}$$

Ist

$$x^{m_\varkappa} \equiv 1 \pmod{r_\varkappa}, \tag{9}$$

so ist $b_\varkappa \equiv p_\varkappa \pmod{r_\varkappa}$, anderseits wegen (7): $b_\varkappa \equiv 0 \pmod{r_\varkappa}$. Daraus folgt

$$r_\varkappa = p_\varkappa, \tag{10}$$

weil $r_\varkappa$ und $p_\varkappa$ Primzahlen sind. Es ist dann

$$p_\varkappa^2 \nmid b_\varkappa. \tag{11}$$

Wegen (9) und (10) ist nämlich $x^{m_\varkappa} = sp_\varkappa + 1$, also

$$b_\varkappa = 1 + (sp_\varkappa + 1) + \cdots + (sp_\varkappa + 1)^{p_\varkappa - 1} = p_\varkappa + Ap_\varkappa^2 \not\equiv 0 \pmod{p_\varkappa^2}.$$

Ist

$$x^{m_\varkappa} \not\equiv 1 \pmod{r_\varkappa}, \tag{12}$$

so folgt nach (8) und dem Fermatschen Satz:

$$x^t \equiv 1 \pmod{r_\varkappa}, \text{ wenn } t = (r_\varkappa - 1, m_\varkappa p_\varkappa) \text{ ist.} \tag{13}$$

Es ist nun auf Grund von (12) $p_\varkappa^{\alpha_\varkappa} \mid t$, also auch ein Teiler von $r_\varkappa - 1$:

$$r_\varkappa \equiv 1 \pmod{p_\varkappa^{\alpha_\varkappa}} \text{ für } \varkappa = 1, \ldots, k. \tag{14}$$

Ist nun r ein Primteiler von $F_m(x)$, so erfüllt r nach (6), (10) und (14) je eine Bedingung aus den folgenden k Paaren von Bedingungen:

$$\begin{aligned} &\text{Entweder } r = p_1 \text{ oder } r \equiv 1 \pmod{p_1^{\alpha_1}} \\ &\qquad\vdots \\ &\text{Entweder } r = p_k \text{ oder } r \equiv 1 \pmod{p_k^{\alpha_k}}. \end{aligned} \tag{15}$$

Weil $p_1, \ldots, p_k$ paarweise verschieden sind, kann dabei die erste Bedingung aus höchstens einem Paare erfüllt sein. Also bestehen für r nur folgende zwei Möglichkeiten:

(16) $r = p_\lambda$ und $r \equiv 1 \pmod{p_\varkappa^{\alpha_\varkappa}}$, wobei λ eine feste unter den Zahlen $1, \ldots, k$ ist und $\varkappa$ diese Zahlen durchläuft, aber $\varkappa \neq \lambda$ ist.

(17) $\qquad r \neq p_\varkappa$ und $r \equiv 1 \pmod{p_\varkappa^{\alpha_\varkappa}} \qquad (\varkappa = 1, \ldots, k).$

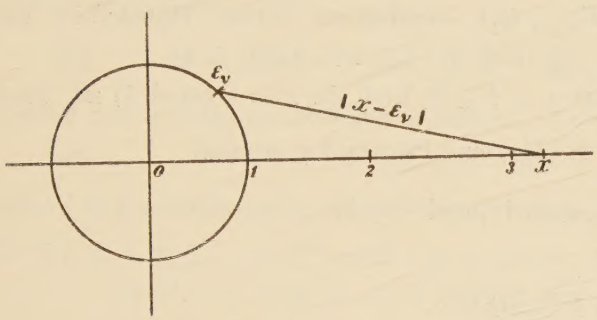
Wegen der Annahme $p_1 < \cdots < p_k$ kann (16) nur im Falle $\lambda = k$ eintreten. (16) und (17) nehmen daher folgende Gestalt an:

(18) $\qquad r = p_k$ und $r \equiv 1 \pmod{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{k-1}^{\alpha_{k-1}}},$

(19) $\qquad r \equiv 1 \pmod{m}.$

Auf Grund von (6) und (11) kann ferner p_k^2 nicht Teiler von $F_m(x)$ sein. Damit ist (2) bewiesen.

Folgerung aus Satz (2): Soll $F_m(x)$ an der ganzen rationalen Stelle $x > 1$ keinen Primteiler besitzen, der $\equiv 1 \pmod{m}$ ist, so kann nur $p_k \mid F_m(x)$ sein, d. h., es ist



(20) $\qquad F_m(x) = p_k.$

Beispiel: $F_6(x) = x^2 - x + 1$.
$F_6(2) = 4 - 2 + 1 = 3$; $m = 6 = 2 \cdot 3$;
$p_k = 3 \equiv 1 \pmod 2$.

(21) **Satz.** *Für $m \geqq 3$ und $x \geqq 3$, x ganz rational, enthält $F_m(x)$ mindestens einen Primteiler, der $\equiv 1 \pmod m$ ist.*

Beweis. $F_m(x)$ ist, wenn x ganz rational ist, eine positive ganze rationale Zahl. Auf Grund von (1) gilt daher auch:

(22) $\qquad F_m(x) = |x - \varepsilon_1| \cdot |x - \varepsilon_2| \cdots |x - \varepsilon_{\varphi(m)}|.$

Wegen $x \geqq 3$ ist nun $|x - \varepsilon_\nu| > 2$ $(\nu = 1, \ldots, \varphi(m))$ (vgl. Zeichnung). Daraus folgt

(23) $\qquad F_m(x) > 2^{\varphi(m)}.$

Weil $\varphi(m) \geqq p_k - 1$, $2^{\varphi(m)} \geqq 2^{p_k - 1} \geqq p_k$ ist, so ergibt sich nach (23) und der Folgerung aus Satz (2) sofort die Behauptung von (21).

II. Eine Beziehung zwischen der größten in einer ungeraden vollkommenen Zahl aufgehenden Primzahl und dem größten bei der Primfaktorenzerlegung auftretenden Exponenten.

(1) **Satz.** *Ist $n = p^\alpha q_1^{2\beta_1} \cdots q_r^{2\beta_r}$ eine ungerade vollkommene Zahl* [4]*, so ist*

$$\operatorname{Max}(p, q_1, \ldots, q_r) > 2 \operatorname{Max}(\alpha + 1, 2\beta_1 + 1, \ldots, 2\beta_r + 1).$$

Beweis. Da für eine vollkommene Zahl (s. Einleitung)

(2) $\qquad \sigma(n) = 2n$

und nach Formeln der elementaren Zahlentheorie

(3) $\qquad \sigma(n) = (1 + p + p^2 + \cdots + p^\alpha) \cdot \prod_{\varrho=1}^{r} (1 + q_\varrho + q_\varrho^2 + \cdots + q_\varrho^{2\beta_\varrho})$

gilt, da ferner $\alpha \equiv 1 \pmod 4$ [5]) ist, so folgt:

(4) $\qquad \frac{1}{2}(1 + p + p^2 + \cdots + p^\alpha) \mid n$

und

[4]) Vgl. Fußnote [1]).
[5]) Vgl. Fußnote [1]).

$$1 + q_\varrho + q_\varrho^2 + \cdots + q_\varrho^{2\beta_\varrho} \mid n \qquad (\varrho = 1, \ldots, r).$$

Es ist

$$(5) \qquad \frac{1}{2}(1 + p + p^2 + \cdots + p^\alpha) =$$

$$\frac{p+1}{2}(1 + p + p^2 + \cdots + p^{\frac{\alpha-1}{2}})(1 - p + p^2 - + \cdots + p^{\frac{\alpha-1}{2}}).$$

Nach I, (3):

$$(6) \qquad \begin{aligned} &F_{\frac{\alpha+1}{2}}(p) \mid 1 + p + p^2 + \cdots + p^{\frac{\alpha-1}{2}}; \\ &F_{\alpha+1}(p) \mid 1 - p + p^2 - + \cdots + p^{\frac{\alpha-1}{2}}; \\ &F_{2\beta_\varrho+1}(q_\varrho) \mid 1 + q_\varrho + q_\varrho^2 + \cdots + q_\varrho^{2\beta_\varrho}. \end{aligned}$$

Auf Grund von I, (21) besitzt $F_{2\beta_\varrho+1}(q_\varrho)$ mindestens einen Primteiler, der $\equiv 1 \pmod{2\beta_\varrho + 1}$, also $\geqq 2(2\beta_\varrho + 1) + 1 > 2(2\beta_\varrho + 1)$ ist. Ist $\operatorname{Max}(\alpha, 2\beta_1, \ldots, 2\beta_r) = \alpha$, so ist $\alpha + 1 \geqq 3$, und, da $\alpha \equiv 1 \pmod 4$ ist, auch $\frac{\alpha+1}{2} \geqq 3$. Es gibt dann, wieder nach I, (21), eine Primzahl q_λ so, daß

$$(7) \qquad q_\lambda \mid F_{\alpha+1}(p), \quad q_\lambda \equiv 1 \pmod{\alpha + 1}$$

ist. Für diese Primzahl q_λ gilt

$$(8) \qquad q_\lambda \nmid F_{\frac{\alpha+1}{2}}(p),$$

weil $q_\lambda \mid F_{\alpha+1}(p)$ besagt:

$$(9) \qquad q_\lambda \mid p^{\frac{\alpha+1}{2}} + 1$$

und $q_\lambda \mid F_{\frac{\alpha+1}{2}}(p)$:

$$(10) \qquad q_\lambda \mid p^{\frac{\alpha+1}{2}} - 1.$$

Wegen (7) ist aber $q_\lambda \neq 2$, und daher können (9) und (10) nicht gleichzeitig bestehen. Es gibt deshalb eine Primzahl q_μ so, daß

$$(11) \qquad q_\mu \neq q_\lambda; \quad q_\mu \mid F_{\frac{\alpha+1}{2}}(p); \quad q_\mu \equiv 1 \left(\operatorname{mod} \frac{\alpha+1}{2}\right)$$

ist. Da $\frac{\alpha+1}{2}$ ungerade ist, so gilt auch:

$$(12) \qquad q_\mu \equiv 1 \pmod{\alpha + 1}.$$

Aus (7), (11) und (12) folgt, daß mindestens eine der beiden Zahlen q_λ, q_μ größer als $2(\alpha + 1)$ ist. Damit ist der Beweis des Satzes (1) zum Abschluß gebracht.

III. Eine Eigenschaft des größten gemeinsamen Teilers der um 1 vermehrten geraden Exponenten in der Primfaktorenzerlegung einer ungeraden vollkommenen Zahl.

(1) **Satz.** *Ist* $n = p^\alpha q_1^{2\beta_1} \cdots q_r^{2\beta_r}$

$$= \frac{p+1}{2}\left(1 + p + \cdots + p^{\frac{\alpha-1}{2}}\right)\left(1 - p + - \cdots + p^{\frac{\alpha-1}{2}}\right) \prod_{\varrho=1}^{r}(1 + q_\varrho + \cdots + q_\varrho^{2\beta_\varrho})$$

eine ungerade vollkommene Zahl, und die beliebige ganze rationale Zahl t ein gemeinsamer Teiler aller Zahlen $2\beta_\varrho + 1$ $(\varrho = 1, \ldots, r)$, so ist mindestens t^4 ein Teiler von n.

Beweis. Es muß gezeigt werden: Ist l eine Primzahl und $l^k \mid 2\beta_\varrho + 1$ $(\varrho = 1, \ldots, r)$, so ist $l^{4k} \mid n$.

A. Zunächst wird bewiesen, daß $l^k \mid n$ ist.

Ist ein q_ϱ, z. B. $q_1 \equiv 1 \pmod{l}$, so ist $l^k \mid n$. Denn es ist

$$(2)\quad 1 + q_1 + q_1^2 + \cdots + q_1^{2\beta_1} = (1 + q_1 + q_1^2 + \cdots + q_1^{l^k-1})(1 + q_1^{l^k} + q_1^{2l^k} + \cdots) \mid n.$$

$$(3)\quad 1 + q_1 + q_1^2 + \cdots + q_1^{l^k-1}$$
$$= (1 + q_1 + \cdots + q_1^{l-1})(1 + q_1^l + \cdots + q_1^{(l-1)l}) \cdots (1 + q_1^{l^{k-1}} + \cdots + q_1^{(l-1)l^{k-1}}).$$

Da jede Klammer der rechten Seite von (3) wegen $q_1 \equiv 1 \pmod{l}$ den Teiler l enthält, so ist $l^k \mid n$. Ist nun

$$(4)\quad q_\varrho \not\equiv 1 \pmod{l} \qquad (\varrho = 1, \ldots, r),$$

so folgt nach I, Satz (2):

$$(5)\quad p \equiv 1 \pmod{l} \text{ und } \prod_{\varrho=1}^{r} (1 + q_\varrho + q_\varrho^2 + \cdots + q_\varrho^{l^k-1}) = p^\xi,$$

wobei ξ eine gewisse positive ganze Zahl ist. Gilt für eine der Zahlen ϱ, z. B. für ν:

$$(6)\quad l \mid 2\beta_\nu + 1 \quad \text{und} \quad s \mid 2\beta_\nu + 1,$$

wobei l und s voneinander verschiedene Primzahlen sind, so ergibt sich:

$$(7)\quad 1 + q_\nu + q_\nu^2 + \cdots + q_\nu^{2\beta_\nu r} = (1 + q_\nu + q_\nu^2 + \cdots + q_\nu^{l-1})(1 + q_\nu^l + q_\nu^{2l} + \cdots + q_\nu^{(s-1)l})(\cdots)$$
$$= (1 + q_\nu + q_\nu^2 + \cdots + q_\nu^{s-1})(1 + q_\nu^s + q_\nu^{2s} + \cdots + q_\nu^{(l-1)s})(\cdots).$$

Da p nach (4) und (5) die einzige in n enthaltene Primzahl ist, die der Restklasse $1 \pmod{l}$ angehört, so folgt aus I, Satz (2):

$$(8)\quad 1 + q_\nu + q_\nu^2 + \cdots + q_\nu^{l-1} = p^{\varkappa_1}.$$

Zu dieser Gleichung tritt eine zweite, die im Falle $q_\nu^s \not\equiv 1 \pmod{l}$ lautet:

$$(8')\quad 1 + q_\nu^s + q_\nu^{2s} + \cdots + q_\nu^{(l-1)s} = p^{\varkappa_2}$$

und im Falle $q_\nu^s \equiv 1 \pmod{l}$:

$$(8'')\quad 1 + q_\nu^s + q_\nu^{2s} + \cdots + q_\nu^{(l-1)s} = lp^{\varkappa_2}.$$

In beiden Fällen ist $\varkappa_2 > \varkappa_1$. Im Falle (8′) ist das selbstverständlich; im Falle (8″) ergibt es sich durch folgenden Schluß: Nach (6) sind l und s beide $\geqq 3$. Setzt man $1 + q_\nu + q_\nu^2 + \cdots + q_\nu^{ls-1} = y^3$, wobei y eine reelle Zahl > 1, aber nicht notwendig ganz ist, so ist nach (8) und (8″): $p^{\varkappa_1} < y$, $lp^{\varkappa_2} > y^2$ und also $lp^{\varkappa_2-\varkappa_1} > y > 1$. Wäre $\varkappa_2 < \varkappa_1$, so wäre, weil $p > l$ ist auf Grund von (5), $lp^{\varkappa_2-\varkappa_1} = \dfrac{l}{p^{\varkappa_1-\varkappa_2}} < 1$, was der obigen Ungleichung widerspricht. Wäre $\varkappa_1 = \varkappa_2$, so würde sich $l > y$ ergeben, was aber (8) und $p^{\varkappa_1} < y$ widerspricht. Aus (8) ergibt sich $q_\nu^l \equiv 1 \pmod{p}$ und daraus auf Grund von (7) und $\varkappa_1 < \varkappa_2$:

$$(9)\quad p \mid 1 + q_\nu^l + q_\nu^{2l} + \cdots + q_\nu^{(s-1)l} \equiv s \pmod{p},$$

also $p \mid s$ und, weil p und s Primzahlen sind:

$$(10)\quad s = p.$$

Dieses Ergebnis besagt nun, daß $\prod_{\varrho=1}^{r} (1 + q_\varrho + q_\varrho^2 + \cdots + q_\varrho^{2\beta_\varrho})$ nur in Klammern zerfällt, die entweder aus l oder p Summanden bestehen. Nach (4), (5) und I, (2) folgt daraus, daß dieses Produkt als Primteiler nur p und Zahlen der Restklasse $1 \pmod{p}$ enthalten kann. Es sei jetzt

$$(11) \qquad q_\lambda \mid \frac{p+1}{2};\ p \equiv -1 \pmod{q_\lambda}.$$

Dann ist $q_\lambda \neq p$, $q_\lambda \not\equiv 1 \pmod{p}$, also:

$$(12) \qquad q_\lambda \nmid \prod_{\varrho=1}^{r} (1 + q_\varrho + q_\varrho^2 + \cdots + q_\varrho^{2\beta_\varrho})$$

und daraus

$$(13) \qquad q_\lambda^{2\beta_\lambda} \mid \frac{p+1}{2}\left(1 + p + p^2 + \cdots + p^{\frac{\alpha-1}{2}}\right)\left(1 - p + p^2 - + \cdots + p^{\frac{\alpha-1}{2}}\right).$$

Wäre $q_\lambda^2 \mid \frac{p+1}{2}$, so ergäbe sich nach (5):

$$(14) \qquad 1 + q_\lambda + q_\lambda^2 + \cdots + q_\lambda^{l-1} = p^{\varkappa_\lambda} \equiv \pm 1 \pmod{q_\lambda^2}.$$

Die linke Seite von (14) ist $\equiv 1 + q_\lambda \pmod{q_\lambda^2}$, die rechte $\equiv \pm 1 \pmod{q_\lambda^2}$. Das liefert einen Widerspruch. $\frac{p+1}{2}$ enthält daher nur Primteiler in der ersten Potenz, d. h.

$$(15) \qquad \frac{p+1}{2} = q_{\lambda_1} q_{\lambda_2} \cdots q_{\lambda_\sigma} \text{ oder } p \equiv -1 \pmod{q_{\lambda_1} q_{\lambda_2} \cdots q_{\lambda_\sigma}}.$$

Auf Grund von (13) und (15):

$$(16) \qquad q_{\lambda_1} q_{\lambda_2} \cdots q_{\lambda_\sigma} \mid 1 - p + p^2 - + \cdots + p^{\frac{\alpha-1}{2}} \equiv \frac{\alpha+1}{2} \pmod{q_{\lambda_1} q_{\lambda_2} \cdots q_{\lambda_\sigma}}.$$

Es ist daher

$$(17) \qquad q_{\lambda_1} q_{\lambda_2} \cdots q_{\lambda_\sigma} \mid \frac{\alpha+1}{2}.$$

Nach II, (6) ist $F_{\frac{\alpha+1}{2}}(p) \mid n$. Nach I, (21) besitzt nun $F_{\frac{\alpha+1}{2}}(p)$ mindestens einen Primteiler q_μ, der $\equiv 1 \left(\mathrm{mod}\ \frac{\alpha+1}{2}\right)$, also nach (17) auch $\equiv 1 \pmod{q_{\lambda_1} q_{\lambda_2} \cdots q_{\lambda_\sigma}}$ ist. Nach (5) und (15) ist mit einer gewissen positiven ganzen Zahl $\varkappa_\mu$:

$$(18) \qquad 1 + q_\mu + q_\mu^2 + \cdots + q_\mu^{l-1} = p^{\varkappa_\mu} \equiv \pm 1 \pmod{q_{\lambda_1} q_{\lambda_2} \cdots q_{\lambda_\sigma}};$$

anderseits ist wegen $q_\mu \equiv 1 \pmod{q_{\lambda_1} q_{\lambda_2} \cdots q_{\lambda_\sigma}}$:

$$(19) \qquad 1 + q_\mu + q_\mu^2 + \cdots + q_\mu^{l-1} \equiv l \pmod{q_{\lambda_1} q_{\lambda_2} \cdots q_{\lambda_\sigma}}.$$

(18) und (19) liefern

$$(20) \qquad l \equiv \pm 1 \pmod{q_{\lambda_1} q_{\lambda_2} \cdots q_{\lambda_\sigma}} \text{ oder } q_{\lambda_1} q_{\lambda_2} \cdots q_{\lambda_\sigma} \mid l^2 - 1.$$

Mit Hilfe von (15) kann man dafür auch schreiben:

$$(21) \qquad \frac{p+1}{2} \mid l^2 - 1.$$

Nach (5) und $p \equiv 1 \pmod 4$ [6]) ist

$$(22) \qquad p \equiv 1 \pmod{4l};\ p = 4cl + 1;\ \frac{p+1}{2} = 2cl + 1.$$

Auf Grund von (21) und (22) ist $l^2 - 1 = f \cdot \frac{p+1}{2} = f(2cl + 1)$. Für f ergibt sich daraus die Bedingung: $f \equiv -1 \pmod{l}$; $f \geqq l - 1$. Das liefert

[6]) Vgl. Fußnote [1]).

$$(23) \qquad l^2 - 1 = (l+1)(l-1) = f(2cl+1) \geqq (l-1)(2cl+1).$$

Da $2cl + 1 > l + 1$ ist, so stellt (23) einen Widerspruch dar. Es ist somit bewiesen, daß $l^k \mid n$ sein muß.

B. Es soll nun gezeigt werden, daß auch $l^{2k} \mid n$ ist.

Die Annahme (4) hat zu einem Widerspruch geführt. Wir können im folgenden daher voraussetzen, daß ein q_ϱ, z. B. $q_1 \equiv 1 \pmod{l}$ ist.

Wir unterscheiden zwei Fälle: (α) $k > 1$; (β) $k = 1$.

(α) $k > 1$. Es ist $l^k \mid 2\beta_\varrho + 1$ ($\varrho = 1, \ldots, r$) nach Voraussetzung. Wegen $q_1 \equiv 1 \pmod{l}$ gilt

$$(24) \quad l^k \mid (1 + q_1 + q_1^2 + \cdots + q_1^{l-1})(1 + q_1^l + q_1^{2l} + \cdots + q_1^{(l-1)l}) \cdots \\ \cdots (1 + q_1^{l^{k-1}} + q_1^{2l^{k-1}} + \cdots + q_1^{(l-1)l^{k-1}}) \mid n.$$

Setzt man zur Abkürzung

$$(25) \quad 1 + q_1 + q_1^2 + \cdots + q_1^{l-1} = a \quad \text{und} \quad 1 + q_1^l + q_1^{2l} + \cdots + q_1^{(l-1)l} = b,$$

so enthält a nach I, (21) einen Primteiler, der $\equiv 1 \pmod{l}$ ist. Dieser Primteiler kann nicht zugleich Teiler von b sein. b ist aber auch durch mindestens eine Primzahl teilbar, die der Restklasse $1 \pmod{l}$ angehört. Das Produkt $a \cdot b$ enthält daher mindestens zwei verschiedene Primteiler, die $\equiv 1 \pmod{l}$ sind. Unter den Zahlen $q_2, q_3, \ldots, q_r$ muß es also mindestens eine geben, die $\equiv 1 \pmod{l}$ ist. Sei $q_2 \equiv 1 \pmod{l}$. Dann folgt

$$(26) \quad l^k \mid (1 + q_2 + q_2^2 + \cdots + q_2^{l-1})(1 + q_2^l + q_2^{2l} + \cdots + q_2^{(l-1)l}) \cdots \\ \cdots (1 + q_2^{l^{k-1}} + q_2^{2l^{k-1}} + \cdots + q_2^{(l-1)l^{k-1}}) \mid n.$$

Aus (24) und (26) ergibt sich: $l^{2k} \mid n$.

(β) $k = 1$. Nehmen wir an, es wäre $l^{2k} \nmid n$; dann würde dies in dem vorliegenden Falle besagen:

$$(27) \qquad l \mid n; \quad l^2 \nmid n.$$

Das heißt, daß $l = p$ sein muß [7]). Wegen $q_1 \equiv 1 \pmod{l}$ ist

$$(28) \qquad l \mid 1 + q_1 + q_1^2 + \cdots + q_1^{l-1} \mid n.$$

$1 + q_1 + q_1^2 + \cdots + q_1^{l-1}$ besitzt wieder nach I, (21) mindestens einen Primteiler $q_2 \equiv 1 \pmod{l}$. Es ist

$$(29) \qquad l \mid 1 + q_2 + q_2^2 + \cdots + q_2^{l-1} \mid n.$$

(28) und (29) liefern einen Widerspruch gegen die Annahme (27). Es ist damit die Behauptung $l^{2k} \mid n$ bewiesen.

C. Um zu zeigen, daß auch $l^{3k} \mid n$ ist, unterscheiden wir drei Fälle:

$$(\alpha)\ k > 2; \quad (\beta)\ k = 2; \quad (\gamma)\ k = 1.$$

(α) $k > 2$. Wir betrachten Formel (24), die auch hier gilt. Wegen $k \geqq 3$ ist nun

$$(30) \qquad 1 + q_1^{l^2} + q_1^{2l^2} + \cdots + q_1^{(l-1)l^2} = c \mid n.$$

Benutzen wir die Abkürzungen (25), so können wir durch dieselben Schlüsse wie oben (vgl. im Anschluß an (25)) sagen: Das Produkt $a \cdot b \cdot c$ enthält mindestens drei verschiedene Primteiler, die $\equiv 1 \pmod{l}$ sind. Unter den Zahlen $q_2, q_3, \ldots, q_r$ gibt es daher mindestens zwei, die $\equiv 1 \pmod{l}$ sind. Seien dies q_2 und q_3. Für q_2 und q_3 gelten Formeln, die sich von (24) nur durch andere Indizes unterscheiden. Es ist deshalb $l^{3k} \mid n$.

(β) $k = 2$. Es ist $l^2 \mid 2\beta_\varrho + 1$, d. h.

---

[7]) Vgl. Fußnote [1]).

$$2\beta_\varrho \geqq 8 \qquad (\varrho = 1, 2, \ldots, r). \tag{31}$$

Wir wissen bereits nach B:

$$l^4 \mid n. \tag{32}$$

$l^{3k} \mid n$ heißt in unserem Falle: $l^6 \mid n$. Ist nun l eine der Zahlen $q_1, q_2, \ldots, q_r$, so ist wegen (31) $l^8 \mid n$, die Behauptung also bewiesen. Ist $l = p$, $q_1 \equiv 1 \pmod{l}$, so gilt, wie im Falle B, (α), daß das Produkt $a \cdot b$ mindestens zwei verschiedene Primteiler der Restklasse 1 (mod l) enthält. Diese sind beide ungleich p. Es gilt deshalb $q_2 \equiv 1 \pmod{l}$ und $q_3 \equiv 1 \pmod{l}$. Daraus folgt wieder wie im vorigen Falle: $l^{3k} \mid n$.

(γ) $k = 1$. Unsere Behauptung lautet: $l^3 \mid n$. Wir unterscheiden die beiden Unterfälle 1. $l > 3$ und 2. $l = 3$.

1. $l > 3$. Weil $l \mid 2\beta_\varrho + 1$ und $l \geqq 5$ ist, folgt

$$2\beta_\varrho \geqq 4 \qquad (\varrho = 1, \ldots, r). \tag{33}$$

Ist l enthalten in $q_1 q_2 \cdots q_r$, so ist nach (33) $l^4 \mid n$. Ist $l = p$, so ist

$$p^\alpha = l^\alpha \mid n; \ \alpha \equiv 1 \pmod 4 \ [8]). \tag{34}$$

Auf Grund von B ist $l^2 \mid n$. Nach (34) folgt: $l^5 \mid n$.

2. $l = 3$. Wegen $p \equiv 1 \pmod 4$ [9]) ist $p \neq 3$. Nehmen wir an, es wäre $3^3 \nmid n$. Dann hätte n die Gestalt

$$n = p^\alpha \cdot 3^2 \cdot q_2^{2\beta_2} \cdot q_3^{2\beta_3} \cdots q_r^{2\beta_r} = \frac{p+1}{2}\left(1 + p + p^2 + \cdots + p^{\frac{\alpha-1}{2}}\right) \tag{35}$$

$$\cdot \left(1 - p + p^2 - + \cdots + p^{\frac{\alpha-1}{2}}\right) \cdot (1 + 3 + 3^2) \cdot \prod_{\varrho=2}^{r} (1 + q_\varrho + q_\varrho^2 + \cdots + q_\varrho^{2\beta_\varrho})$$

$$\text{mit} \qquad 3 \mid 2\beta_\varrho + 1 \qquad (\varrho = 2, 3, \ldots, r).$$

Es ist $1 + 3 + 3^2 = 13 \mid n$.

Ist $p = 13$, so ist $\dfrac{p+1}{2} = 7 \mid n$ und

$$1 + 7 + 7^2 = 3 \cdot 19 \mid n,$$

$$1 + 19 + 19^2 = 3 \cdot 127 \mid n,$$

$$1 + 127 + 127^2 \mid n, \text{ anderseits } \equiv 0 \pmod 3,$$

d. h., es ist mindestens $3^3 \mid n$.

Ist $p \neq 13$, so folgt $1 + 13 + 13^2 = 3 \cdot 61 \mid n$. Aus $p = 61$ ergibt sich nun: $\dfrac{p+1}{2} = 31 \mid n$; $1 + 31 + 31^2 = 3 \cdot 331 \mid n$; $1 + 331 + 331^2 \equiv 0 \pmod 3$

und daraus wieder $3^3 \mid n$.

Ist $p \neq 61$, so ist $1 + 61 + 61^2 = 3 \cdot 13 \cdot 97 \mid n$. Wäre $p = 97$, dann wäre auch

$$\frac{p+1}{2} = 7^2 \mid n; \ 1 + 7 + 7^2 = 3 \cdot 19 \mid n, \text{ d. h. } 3^3 \mid n.$$

Es bleibt somit nur der Fall $p \neq 97$ übrig. Dann folgt aber aus $1 + 97 + 97^2 \equiv 0 \pmod 3$ wieder $3^3 \mid n$. Die Annahme $3^3 \nmid n$ hat zu einem Widerspruch geführt. Der Fall C ist damit erledigt. Es ist $l^{3k} \mid n$.

D. Zum Schluß soll nun gezeigt werden, daß auch $l^{4k} \mid n$ ist. Dazu unterscheiden wir die vier Fälle: (α) $k > 3$; (β) $k = 3$; (γ) $k = 2$; (δ) $k = 1$.

[8]) Vgl. Fußnote [1]).

[9]) Vgl. Fußnote [1]).

(α) $k > 3$. Wir gehen wieder von (24) aus. Wegen $k \geqq 4$ ist

$$1 + q_1^{l^3} + q_1^{2l^3} + \cdots + q_1^{(l-1)l^3} = d \mid n. \tag{36}$$

Benutzen wir die Abkürzungen (25) und (30), so können wir ebenso wie früher sagen: Das Produkt $a \cdot b \cdot c \cdot d$ enthält mindestens vier verschiedene Primteiler, die $\equiv 1 \pmod{l}$ sind. Unter den Zahlen $q_2, q_3, \ldots, q_r$ gibt es daher mindestens drei, die $\equiv 1 \pmod{l}$ sind, und daraus folgt wieder, daß $l^{4k} \mid n$ sein muß.

(β) $k = 3$. Die Behauptung lautet in diesem Falle: $l^{12} \mid n$. Nach Voraussetzung ist $l^3 \mid 2\beta_\varrho + 1$, also

$$2\beta_\varrho \geqq 26 \qquad (\varrho = 1, 2, \ldots, r). \tag{37}$$

Ist l enthalten in $q_1 q_2 \cdots q_r$, so ist nach (37) $l^{26} \mid n$. Ist $l = p$, dann kann man so schließen: Das Produkt $a \cdot b \cdot c$ enthält mindestens drei verschiedene Primteiler, die $\equiv 1 \pmod{l}$ sind und in $q_2 q_3 \cdots q_r$ enthalten sein müssen. Dies liefert die Behauptung.

(γ) $k = 2$: Die Voraussetzung $l^2 \mid 2\beta_\varrho + 1$ liefert

$$2\beta_\varrho \geqq 8 \qquad (\varrho = 1, 2, \ldots, r). \tag{38}$$

Ist l eine der Zahlen $q_1, q_2, \ldots, q_r$, so ist nach (38) $l^8 \mid n$, die Behauptung also bewiesen.

Ist $l = p$, so muß wegen $\alpha \equiv 1 \pmod 4$ [10]) und C mindestens $l^9 \mid n$ sein.

(δ) $k = 1$: Nach C ist $l^3 \mid n$. Ist nun $l = p$, so folgt aus $\alpha \equiv 1 \pmod 4$:

$$l^5 \mid n.$$

Ist l enthalten in $q_1 q_2 \cdots q_r$, so ist $l^4 \mid n$ auf Grund der Strukturformel für ungerade vollkommene Zahlen [11]). Der Beweis von (1) ist damit beendet.

IV. Notwendige Bedingungen für die Exponenten in der Primfaktorenzerlegung einer ungeraden vollkommenen Zahl.

(1) **Satz.** *Ist* $n = p^\alpha q_1^{2\beta_1} q_2^{2\beta_2} \cdots q_r^{2\beta_r}$ *und* $2\beta_\varrho + 1 = l^{\xi_\varrho}$ $(\varrho = 1, \ldots, r)$, *wobei* l *eine Primzahl ist und die* ξ_ϱ *beliebige positive ganze Zahlen bedeuten, so sind die beiden Bedingungen*

$$p \equiv 1 \pmod{l}, \tag{a}$$

$$\frac{\alpha + 1}{2} \equiv 0 \pmod{l} \text{ oder } \frac{\alpha + 1}{2} \equiv 1 \pmod{l} \tag{b}$$

notwendig dafür, daß n *vollkommen ist.*

Beweis. Aus $2\beta_\varrho + 1 = l^{\xi_\varrho}$ folgt

$$2\beta_\varrho = l^{\xi_\varrho} - 1 \quad \text{und} \quad l - 1 \mid 2\beta_\varrho \qquad (\varrho = 1, \ldots, r). \tag{2}$$

Auf Grund von III, (1) ist $l^4 \mid n$. Wäre $p = l$, so wäre wegen (2):

$$\frac{n}{l^\alpha} = q_1^{2\beta_1} q_2^{2\beta_2} \cdots q_r^{2\beta_r} \equiv 1 \pmod{l}. \tag{3}$$

Anderseits wäre aber

$$\frac{n}{l^\alpha} = \frac{l+1}{2}\left(1 + l + l^2 + \cdots + l^{\frac{\alpha-1}{2}}\right)\left(1 - l + l^2 - + \cdots + l^{\frac{\alpha-1}{2}}\right) \cdot \frac{\prod_{\varrho=1}^{r}(1 + q_\varrho + q_\varrho^2 + \cdots + q_\varrho^{2\beta_\varrho})}{l^\alpha} \equiv \frac{l+1}{2} \pmod{l}, \tag{4}$$

[10]) Vgl. Fußnote [1]).

[11]) Vgl. Fußnote [1]).

weil $\prod_{\varrho=1}^{r}(1+q_\varrho+q_\varrho^2+\cdots+q_\varrho^{2\beta_\varrho})$ wegen (2) und I, (2) außer l nur Primteiler der Restklasse 1 (mod l) enthält. (3) und (4) liefern $1 \equiv \frac{l+1}{2} \pmod{l}$, also einen Widerspruch. Daher ist

$$p \neq l. \tag{5}$$

Weil $p^\alpha \mid \prod_{\varrho=1}^{r}(1+q_\varrho+q_\varrho^2+\cdots+q_\varrho^{2\beta_\varrho})$ sein muß, kann, auf Grund von I, (2) und IV, (2) nur noch

$$p \equiv 1 \pmod{l} \tag{6}$$

sein. Für n ergibt sich also

$$n = p^\alpha q_1^{2\beta_1} q_2^{2\beta_2} \cdots q_r^{2\beta_r} = \frac{p+1}{2}\left(1+p+p^2+\cdots+p^{\frac{\alpha-1}{2}}\right) \tag{7}$$

$$\cdot\left(1-p+p^2-+\cdots+p^{\frac{\alpha-1}{2}}\right)\cdot\prod_{\varrho=1}^{r}(1+q_\varrho+q_\varrho^2+\cdots+q_\varrho^{2\beta_\varrho})$$

mit $p \equiv 1 \pmod{l}$, $q_1 = l$ und $2\beta_\varrho + 1 = l^{\delta_\varrho}$ $(\varrho = 1, \ldots, r)$.

Es folgt daraus

$$\frac{n}{l^{2\beta_1}} \equiv 1 \pmod{l}. \tag{8}$$

Ist nun

$$l \mid 1+p+p^2+\cdots+p^{\frac{\alpha-1}{2}} \equiv \frac{\alpha+1}{2} \pmod{l}, \tag{9}$$

so bedeutet dies

$$\frac{\alpha+1}{2} \equiv 0 \pmod{l}. \tag{10}$$

Ist

$$l \nmid 1+p+p^2+\cdots+p^{\frac{\alpha-1}{2}}, \tag{11}$$

so muß auf Grund von (7) und (8)

$$\frac{\alpha+1}{2} \equiv 1 \pmod{l} \tag{12}$$

sein. Der Beweis ist damit beendet. (1) besagt, daß z. B. $n = p^5 q_1^6 q_2^6 \cdots q_r^6$ nicht vollkommen sein kann.

(13) *Die ungerade Zahl $n = p^\alpha q_1^4 q_2^4 \cdots q_r^4$ ist nicht vollkommen.*

Beweis. Nach III, (1) ist $5^4 \mid n$. Nach (1) ist $p \equiv 1 \pmod 5$, also $p \neq 5$. Wir können daher $n = p^\alpha 5^4 q_2^4 \cdots q_r^4$ setzen und sogar noch etwas allgemeiner behaupten:

(14) $n = p^\alpha 5^4 q_2^{2\beta_2} q_3^{2\beta_3} \cdots q_r^{2\beta_r}$ *mit* $2\beta_\varrho + 1 = 5^{\delta_\varrho}$ $(\varrho = 2, 3, \ldots, r)$ *ist nicht vollkommen.*

Es ist $1+5+\cdots+5^4 = 11 \cdot 71 \mid n$. Wegen $p \equiv 1 \pmod 4$ [12]) gilt: $p \neq 11, \neq 71$. Daher ist

(15) $1+11+\cdots+11^4 = 5 \cdot 3221 \mid n$; $1+71+\cdots+71^4 = 5 \cdot 11 \cdot 211 \cdot 2221 \mid n$.

Weil $211 \equiv 3 \pmod 4$ ist, so können wir jetzt n in der Gestalt annehmen:

$$n = p^\alpha 5^4 \cdot 11^{2\beta_2} \cdot 71^{2\beta_3} \cdot 211^{2\beta_4} \cdot q_5^{2\beta_5} \cdots q_r^{2\beta_r}. \tag{16}$$

[12]) Vgl. Fußnote [1]).

Ferner sind noch $2221 \mid n$ und $3221 \mid n$. Mindestens eine dieser beiden Zahlen muß p sein, denn sonst wäre

$$(17)\qquad \begin{aligned} &5 \mid 1 + 211 + \cdots + 211^4 \mid n;\\ &5 \mid 1 + 2221 + \cdots + 2221^4 \mid n;\\ &5 \mid 1 + 3221 + \cdots + 3221^4 \mid n. \end{aligned}$$

(15) und (17) würden dann $5^5 \mid n$ ergeben, entgegen (14).

Ist $p = 2221$, so ist $\dfrac{p+1}{2} = 1111 = 11 \cdot 101 \mid n$, d. h.

$$(18)\qquad 101 \mid n.$$

Daraus folgt

$$(19)\qquad \begin{aligned} &5 \mid 1 + 211 + \cdots + 211^4 \mid n;\ 5 \mid 1 + 101 + \cdots + 101^4 \mid n;\\ &5 \mid 1 + 3221 + \cdots + 3221^4 \mid n. \end{aligned}$$

(15) und (19) liefern wieder $5^5 \mid n$.

Ist $p = 3221$, so ist $\dfrac{p+1}{2} = 1611 = 9 \cdot 179 \mid n$. Es ist dann mindestens $3^4 \mid n$; außerdem ist noch $5^4 \mid n$ und mindestens $11^4 \mid n$. Das liefert

$$(20)\qquad \frac{\sigma(n)}{n} > \frac{11^2}{3^4} \cdot \frac{11 \cdot 71}{5^4} \cdot \frac{5 \cdot 3221}{11^4} = \frac{3221 \cdot 71}{81 \cdot 125 \cdot 11} = \frac{228\,691}{111\,375} > 2.$$

Die Richtigkeit der Behauptungen (13) und (14) ist also erwiesen.

(21) **Satz.** *Ist $n = p^\alpha q_1^{2\beta_1} \cdots q_r^{2\beta_r}$ eine ungerade Zahl, und haben die um 1 vermehrten geraden Exponenten den gemeinsamen Teiler $3 \cdot 3$ oder $3 \cdot 5$ oder $3 \cdot 7$ oder $3 \cdot 11$, so ist n nicht vollkommen. Für den Fall $p = 5$ ist n ebenfalls nicht vollkommen, wenn 3 oder 5 oder 7 gemeinsamer Teiler der Zahlen $2\beta_\varrho + 1$ $(\varrho = 1, \ldots, r)$ ist. Ist $p = 13$ oder 29, so genügt schon die Voraussetzung $3 \mid 2\beta_\varrho + 1$ $(\varrho = 1, \ldots, r)$, ist $p = 17$, die Voraussetzung $5 \mid 2\beta_\varrho + 1$ $(\varrho = 1, \ldots, r)$, um zu zeigen, daß n nicht vollkommen sein kann.*

Beweis.

(a) Es sei zuerst vorausgesetzt, daß $3 \cdot 3 \mid 2\beta_\varrho + 1$ $(\varrho = 1, \ldots, r)$ ist. Dann ist nach III, (1): $3^8 \mid n$ und wegen $p \equiv 1 \pmod 4$ [13]): $p \neq 3$, also $1 + 3 + 3^2 = 13 \mid n$. Wir unterscheiden die Fälle: $(\alpha)\ p = 13$ und $(\beta)\ p \neq 13$.

$(\alpha)\ p = 13$. Es ist $\dfrac{p+1}{2} = 7 \mid n$; $1 + 7 + 7^2 = 3 \cdot 19 \mid n$; $1 + 19 + 19^2 = 3 \cdot 127 \mid n$; $1 + 127 + 127^2 = 3 \cdot 5419 \mid n$; $5419 \equiv -6 \pmod{31}$, d. h. $1 + 5419 + 5419^2 \equiv 0 \pmod{31}$, also $31 \mid n$. Daraus ergibt sich nun:

$$\frac{\sigma(n)}{n} > \frac{1 + 3 + 3^2 + 3^3 + 3^4}{3^4} \cdot \frac{1 + 13}{13} \cdot \frac{1 + 7 + 7^2}{7^2} \cdot \frac{1 + 19 + 19^2}{19^2} \cdot \frac{1 + 31 + 31^2}{31^2} \cdot \frac{128}{127}$$

$$= \frac{11^2 \cdot 14 \cdot 3 \cdot 19 \cdot 3 \cdot 127 \cdot 3 \cdot 331 \cdot 128}{3^4 \cdot 13 \cdot 7^2 \cdot 19^2 \cdot 31^2 \cdot 127} = 2\,\frac{121 \cdot 331 \cdot 128}{3 \cdot 13 \cdot 7 \cdot 19 \cdot 31^2} = 2\,\frac{5\,126\,528}{4\,984\,707} > 2.$$

$(\beta)\ p \neq 13$. Dann ist $1 + 13 + 13^2 = 3 \cdot 61 \mid n$.

Ist $p = 61$, so folgt: $\dfrac{p+1}{2} = 31 \mid n$; $1 + 31 + 31^2 = 3 \cdot 331 \mid n$; $331 \equiv 2 \pmod 7$, d. h. $1 + 331 + 331^2 \equiv 0 \pmod 7 : 7 \mid n$; $1 + 7 + 7^2 = 3 \cdot 19 \mid n$. Daraus folgt wieder $\dfrac{\sigma(n)}{n} > 2$.

[13]) Vgl. Fußnote [1]).

Ist $p \neq 61$, so ist $1 + 61 + 61^2 = 3 \cdot 13 \cdot 97 \mid n$. Nun ist $61 \equiv 4 \pmod{19}$; $61^3 \equiv 7 \pmod{19}$, also $1 + 61^3 + 61^6 \equiv 0 \pmod{19}$; $19 \mid n$; $127 \mid n$; $5419 \mid n$; $31 \mid n$; $331 \mid n$; $7 \mid n$; schließlich $\frac{\sigma(n)}{n} > 2$.

(b) Es sei jetzt $3 \cdot 5 \mid 2\beta_\varrho + 1$ $(\varrho = 1, \ldots, r)$.

Nach III, (1) folgt: $3^4 \mid n$ und $5^4 \mid n$. Ferner ist $1 + 3 + 3^2 + 3^3 + 3^4 = 11^2 \mid n$; $1 + 11 + 11^2 = 7 \cdot 19 \mid n$. Daraus: $\frac{\sigma(n)}{n} > 2$.

(c) Ist $3 \cdot 7 \mid 2\beta_\varrho + 1$ $(\varrho = 1, \ldots, r)$, so ist $3 \mid n$; $7 \mid n$; $13 \mid n$; $19 \mid n$; $127 \mid n$; $5419 \mid n$; $31 \mid n$; $\frac{\sigma(n)}{n} > 2$.

(d) Ist $3 \cdot 11 \mid 2\beta_\varrho + 1$ $(\varrho = 1, \ldots, r)$, so ist $3 \mid n$; $11 \mid n$; $13 \mid n$; $7 \mid n$; $19 \mid n$; $\frac{\sigma(n)}{n} > 2$.

(e) Ist nun $p = 5$ und $3 \mid 2\beta_\varrho + 1$ $(\varrho = 1, \ldots, r)$, so folgt nach III, (1), daß mindestens $3^4 \mid n$ ist. Auf Grund von $3 \mid 2\beta_\varrho + 1$ ist dann aber mindestens $3^8 \mid n$. Ferner ergibt sich wieder: $13 \mid n$; $61 \mid n$; $97 \mid n$; $3169 \mid n$;

$$\frac{\sigma(n)}{n} \geqq \frac{1 + 3 + \cdots + 3^8}{3^8} \cdot \frac{1 + 5}{5} \cdot \frac{1 + 13 + 13^2}{13^2} \cdot \frac{1 + 61 + 61^2}{61^2} \cdot \frac{1 + 97 + 97^2}{97^2}$$

$$\cdot \frac{1 + 3169 + 3169^2}{3169^2} = \frac{13 \cdot 757}{3^8} \cdot \frac{6}{5} \cdot \frac{3 \cdot 61}{13^2} \cdot \frac{3 \cdot 13 \cdot 97}{61^2} \cdot \frac{3 \cdot 3169}{97^2} \cdot \frac{3 \cdot 3\,348\,577}{3169^2}$$

$$= 2 \cdot \frac{757 \cdot 3\,348\,577}{3^3 \cdot 5 \cdot 61 \cdot 97 \cdot 3169} = 2 \cdot \frac{2\,534\,872\,789}{2\,531\,381\,355} > 2.$$

(f) Vorausgesetzt sei: $p = 5$ und $5 \mid 2\beta_\varrho + 1$ $(\varrho = 1, \ldots, r)$.

Es ist $\frac{p+1}{2} = 3 \mid n$; $1 + 3 + 3^2 + 3^3 + 3^4 = 11^2 \mid n$; nach III, (1): $5^4 \mid n$ und daraus nach (20): $\frac{\sigma(n)}{n} > 2$.

(g) Ist $p = 5$ und $7 \mid 2\beta^\varrho + 1$ $(\varrho = 1, \ldots, r)$, so folgt wegen $3 \mid n$; $5 \mid n$; $7 \mid n$: $\frac{\sigma(n)}{n} > 2$.

(h) Voraussetzung: $p = 13$; $3 \mid 2\beta_\varrho + 1$ $(\varrho = 1, \ldots, r)$.
Der Beweis dieses Falles ist in (a), (α) enthalten.

(i) Ist $p = 29$ und $3 \mid 2\beta_\varrho + 1$ $(\varrho = 1, \ldots, r)$, so ergibt sich:
$\frac{p+1}{2} = 3 \cdot 5 \mid n$; $1 + 5 + 5^2 = 31 \mid n$; $331 \mid n$; $7 \mid n$; $\frac{\sigma(n)}{n} > 2$.

(k) Ist $p = 17$ und $5 \mid 2\beta_\varrho + 1$ $(\varrho = 1, \ldots, r)$, dann folgt:
$\frac{p+1}{2} = 3^2 \mid n$; $1 + 3 + 3^2 + 3^3 + 3^4 = 11^2 \mid n$; also nach III, (1) und (20): $\frac{\sigma(n)}{n} > 2$.

Lebenslauf.

Am 29. Juli 1914 wurde ich, Hans-Joachim Kanold, als Sohn des Kaufmanns Bruno Kanold und seiner Ehefrau Hedwig, geb. Stasch, in Breslau geboren. Nachdem ich Ostern 1933 die Reifeprüfung am Reformrealgymnasium zum Heiligen Geist in Breslau abgelegt und anschließend das freiwillige Werkhalbjahr abgeleistet hatte, nahm ich im Wintersemester 1933/34 an der Universität Breslau das Studium der Mathematik, Physik und Chemie auf. Die mündliche Doktorprüfung bestand ich am 20. 9. 1939 vor der Naturwissenschaftlichen Fakultät Breslau. Seit dem 15. Januar 1940 bin ich bei der Fa. Messerschmitt A.-G. in Augsburg als Mathematiker tätig.

Meine akademischen Lehrer sind: Bergmann, Cramer, Feigl, Fues, Julius Meyer, Radon, Schaefer, Tautz.

Ich möchte an dieser Stelle meinem hochverehrten Lehrer, Herrn Prof. Dr. Feigl, meinen tiefempfundenen Dank aussprechen für die vielen Anregungen, die er mir in den Jahren meines Studiums gegeben, und für die vielen Mühen, die er meinetwegen auf sich genommen hat.

Hans-Joachim Kanold.